pwc

2024 Digital Trust Insights: Middle East findings

Putting security at the epicentre of innovation

The 2024 Global Digital Trust Insights survey of 3,876 business and tech executives at some of the largest global companies, including 110 respondents from across the Middle East, looks at critical cyber risk concerns, the need to place controls everywhere (including identity and access) and the excitement around Generative AI, bringing new threats as well as unprecedented promise for defence.

Both globally and regionally we find breach costs and the number of high-dollar breaches on the rise. Although cloud attacks are the top cyber concern, about one-third of organisations have no risk management plan to address cloud service provider challenges. Only half are 'very satisfied' with their technology capabilities in key cybersecurity areas and more than 30% of companies don't consistently follow what should be standard practices of cyber defence. So that implies that there is room for improvement.

In the Middle East as companies pivot more toward digital business models, more data is generated and shared among organisations, partners and customers. Increasing digitisation means companies are exposed to new digital vulnerabilities, making an effective approach to cybersecurity and digital trust more important than ever.

At the 2023 Gulf Information Security Expo and Conference earlier this year, it was revealed that the region's cybersecurity market, **valued at US$7.5 billion in 2022, is expected to grow at a compound annual growth rate of nearly 20 per cent over the next seven years.** Leading the sector will be countries such as the UAE and Saudi Arabia, owing to their robust cybersecurity industries and government policies that makes them preferred destinations for industry academics, businesses, research and innovation.

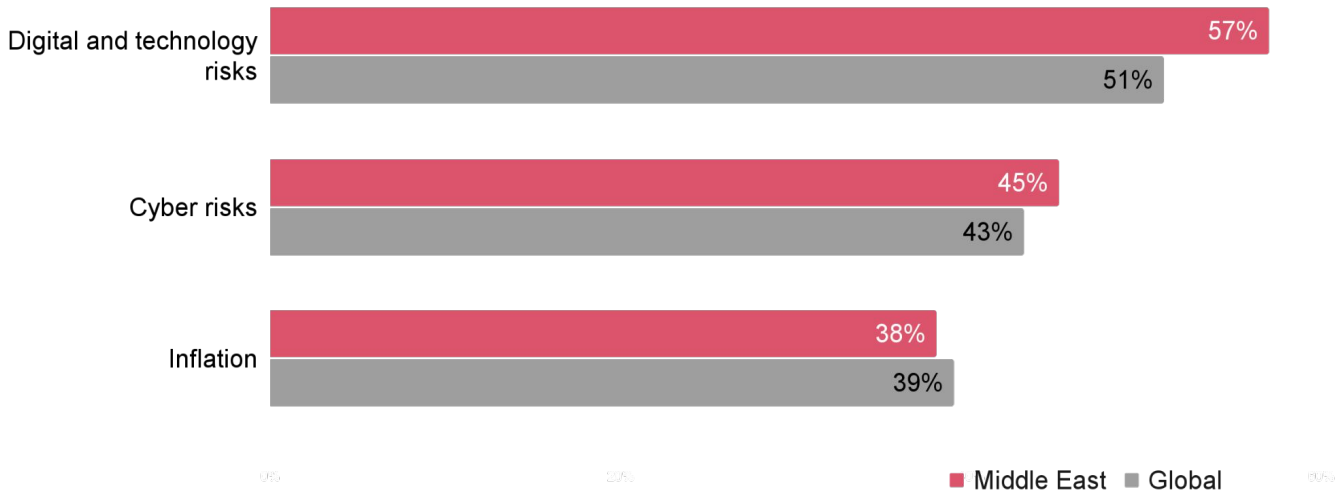
Our survey has highlighted the positive cybersecurity technology solution sentiment in the region, with 77% of regional respondents saying they have the right amount of cybersecurity technology solutions compared to 69% globally, while 14% said they have too many cybersecurity technology solutions and would like to consolidate into cohesive suites to avoid big, costly breaches, compared to 19% globally.

Cyber risk management: Ripe for reinvention

Mitigating cyber risk remains a top priority for Middle Eastern organisations, as revealed by 45% of respondents in the region (vs 43% globally), higher than microeconomic volatility, inflation and geopolitical risks. After dropping to fourth place in last year's **PwC Annual Global CEO Survey**, it's now second for our respondents, behind only digital and technology risks on the list of prioritised risks. And in the minds of our respondents, digital and technology risks are inextricable from cyber risk.

In today's business climate, digital transformation or reinvention cannot be discussed without spotlighting on key cyber threats. In fact, there's nothing more empowering than knowing that governments have innovated and taken bold moves to remain safe and secure.

The Middle East's strong economic growth, improved cyber awareness and the investments being made to protect critical infrastructure have made it resilient to cyber attacks that continue to be more sophisticated and advanced.

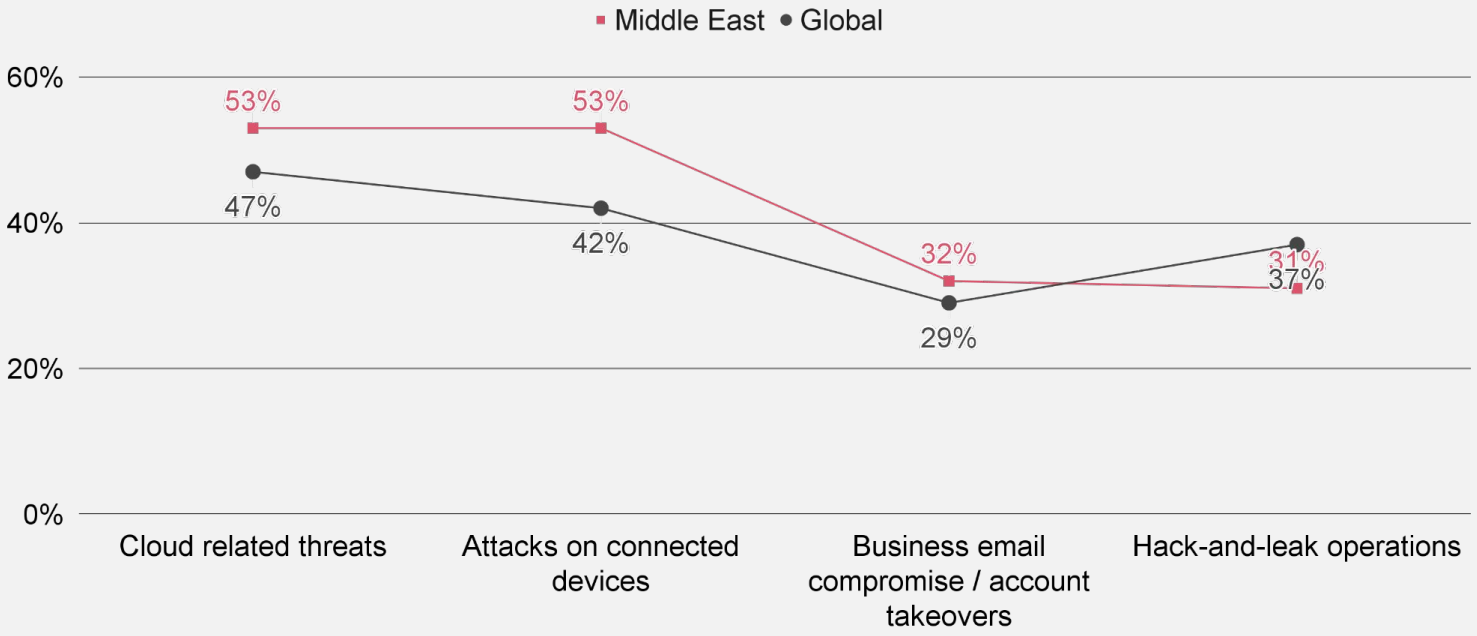


Question: Which of the following risks is your organisation prioritising for mitigation over the next 12 months?
Base: Global respondents = 3876, Middle East respondents = 110
Source: PwC, 2024 Global Digital Trust Insights

Digital tops the risk list in two ways

Aligned to the Global findings, in the Middle East digital and technology risks have topped the list when it comes to the risks organisations are prioritising for mitigation over the next 12 months (57%) as well the risks most connected to an organisation's cyber risks (69%).

Cloud attacks (42% global and 53% in the ME) and attacks on connected devices (47% global and 53% in the ME) are the cyber threats survey respondents are most concerned about — two technologies at the heart of business transformation today. There is a slight difference when it comes to the third cyber threat - hack-and-leak operations for global (37%), while business email compromise for the ME (32%).



Question: Which of the following proposed regulatory goals and principles will have the greatest impact on your organisation's ability to secure future revenue growth?
Base: Global respondents = 3876, Middle East respondents = 110
Source: PwC, 2024 Global Digital Trust Insights

Everything is connected, including cyber attacks

Cyber threats are interconnected and inter-related. When malicious actors break into systems and networks, they often cause damages in multiple ways. What may start as a cloud breach could very well become an advanced persistent threat as bad actors lurk inside the system, exfiltrating the data, launching a ransomware attack, and then finally leaking the data ("hack and leak") even if you pay the ransom.

Middle East respondents revealed that loss of revenue (in terms of lost contracts, lost business opportunities) was the top concern for the outcomes of potential cyber attack in the next 12 months (51% vs 48% globally), followed by loss of customer, employee or transaction data (45% vs 52% globally) and damage to the company brand, including loss of customer confidence (44% vs 50% globally). Any one of these incidents would be problematic on its own. Taken all together, they can devastate business operations and reputation.

Breaches are becoming more costly

Mega breaches are increasing in number and scale — and cost.

Globally, the percentage of organisations reporting costs of $1 million or more for their worst breach in the past three years rose to 36% from 27% last year. The corresponding number this year for organisations in the Middle East is 29%.

19%

of the Middle East respondents estimate the cost of their most damaging data breach between US$1 million - US$9 million

8%

of the Middle East respondents estimate the cost of their most damaging data breach between US$10 million - US$19 million

2%

of the Middle East respondents estimate the cost of their most damaging data breach at US$20 million or more

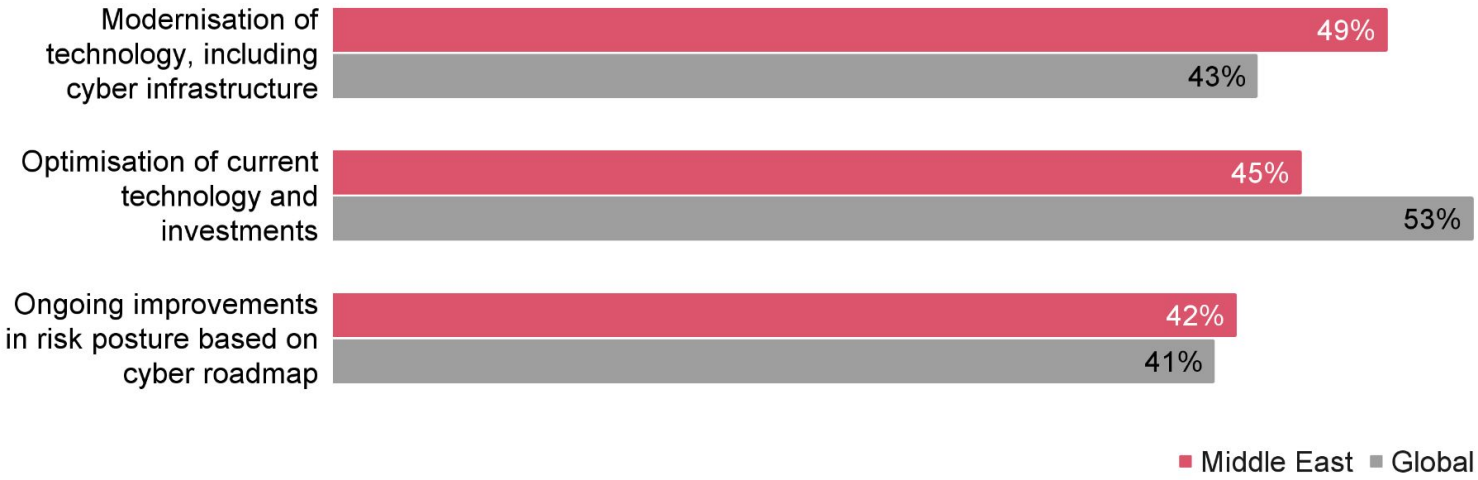
Question: Thinking about the most damaging data breach you experienced in the past three years, please provide an estimate of the cost to your organisation
Base: Middle East respondents = 48
Source: PwC, 2024 Global Digital Trust Insights

Cyber-investment priorities for 2024

Modernisation and optimisation top the cyber-investment priorities for 2024. When asked which investments would be prioritised when allocating your organisation's cyber budget in the next 12 months, more than half (53%) of our regional respondents chose optimisation of existing technologies and investments in order to identify those with the highest potential to create value, while 43% selected technology modernisation, including cyber infrastructure.

Globally it has been the opposite, with nearly half (49%) of the business leaders globally selected technology modernisation as their priorities, including cyber infrastructure, and 45% chose optimisation of existing technologies and investments.

Top three cybersecurity investment priorities over the next 12 months



Question: Which of the following investments are you prioritising when allocating your organisation's cyber budget in the next 12 months?
Base: Global respondents = 1925, Middle East respondents 49
Source: PwC, 2024 Global Digital Trust Insights

When asked about their organisation's technology capabilities, regional survey respondents revealed that firewall/VPN technologies (72%) and cloud security (70%) topped their list.

69% of respondents also revealed that their organisation was planning to prioritise upskilling the current workforce fast enough to keep up with demands of the organisation over the next 12 months, same as the global.

This echoes PwC's latest **Global Annual CEO survey**, where 66% of Middle East CEOs said they hope to deploy cloud technology, artificial intelligence, and other advanced technology in operations. Improving workforce skills is a critical component of this digital transformation, with 74% of Middle East CEOs keen to invest in reskilling their workforce.

Cloud security: Overdue for concerted attention

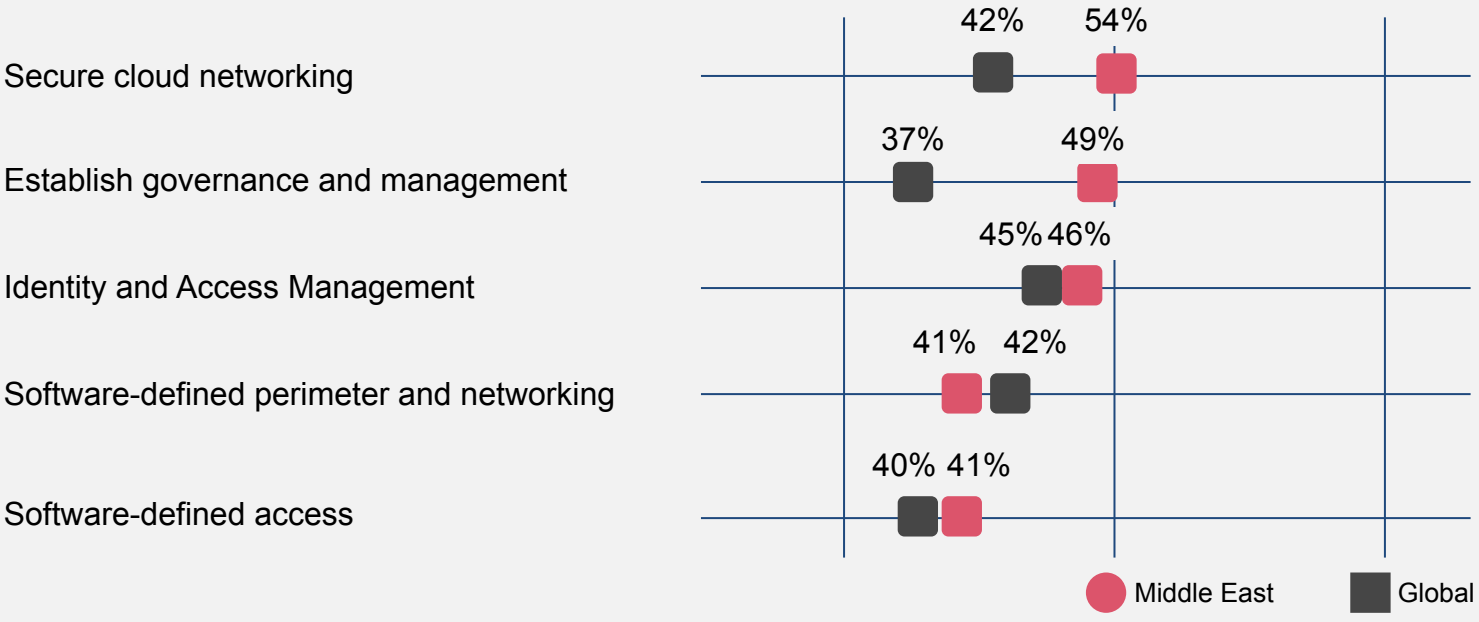
As businesses push the boundaries of innovation, it enables developers to collaborate no matter where in the world they might be; adopting new, more flexible ways to work; inventing new business models; connecting technologies to help better operate the business; providing superior service to customers and clients; and so on.

Migration to the cloud has increased in the region, and the demand has been growing steadily among financial services organisations, making it a key point of discussion in the transformation agenda, according to PwC's recent **Cloud Business Survey**. Understandably, cloud security remains the top cyber risk concern for more at 53% respondents across the Middle East, compared to 47% globally.

Bad actors have potentially limitless ways to enter an organisation's system(s) and therefore, it is critical to place controls everywhere: on identity and access, lateral movement, email accounts, website portals, applications, proprietary information, customer interactions, operating systems, connected devices. However, less than half (49%) of Middle East respondents prioritised cloud security investments when allocating the organisation's cyber budget in the next 12 months, compared to 33% globally. The other investment priorities remained network security (31% vs 28% globally) and application security (30% vs 31% globally).

Highlighting their organisation's top priorities in the next 12 months as it shifts to a zero trust mode, 54% of regional respondents said it would be secure cloud networking (as against 42% globally), while 46% said it would be identity and access management, almost the same as global respondents.

Percentage who say this is their organisation's top priorities in the next 12 months



Question: What are your organisation's top priorities in the next 12 months as your organisation shifts to a zero trust concept?
Base: Global respondents = 1434, Middle East respondents = 41
Source: PwC, 2024 Global Digital Trust Insights

Generative AI for cyber defence on the rise

As the size of the global digital economy is growing and expanding, and is expected to reach around US$20 trillion in 2025, the size of cybercrime is increasing, leading to global economic losses estimated at around 40% of the size of the digital economy and is expected to increase. Large Language Models of GenAI can be formidable weapons to expedite cyber threat detection and the initial response while simplifying the complex data analysis and security engineering processes.

Our survey has revealed that 83% respondents in the region vs more than 77% globally strongly agree that their leadership is focused on ethical and responsible use of generative AI tools, while 89% agree that Generative AI will help their organisation develop new lines of business within the next 3 years against 77% globally.

Many vendors are pushing the limits of GenAI, testing what's possible. It could be some time before we see broad-scale use of defenceGPTs. In the meantime, here are the three most promising areas for using GenAI in cyber defence.

01

Threat detection and analysis:
GenAI can be invaluable for proactively detecting vulnerability exploits, rapidly assessing their extent — what's at risk, what's already compromised and what the damages are, and then presenting tried-and-true options for defence and remediation. GenAI can identify patterns, anomalies and indicators of compromise that elude traditional signature-based detection systems.

02

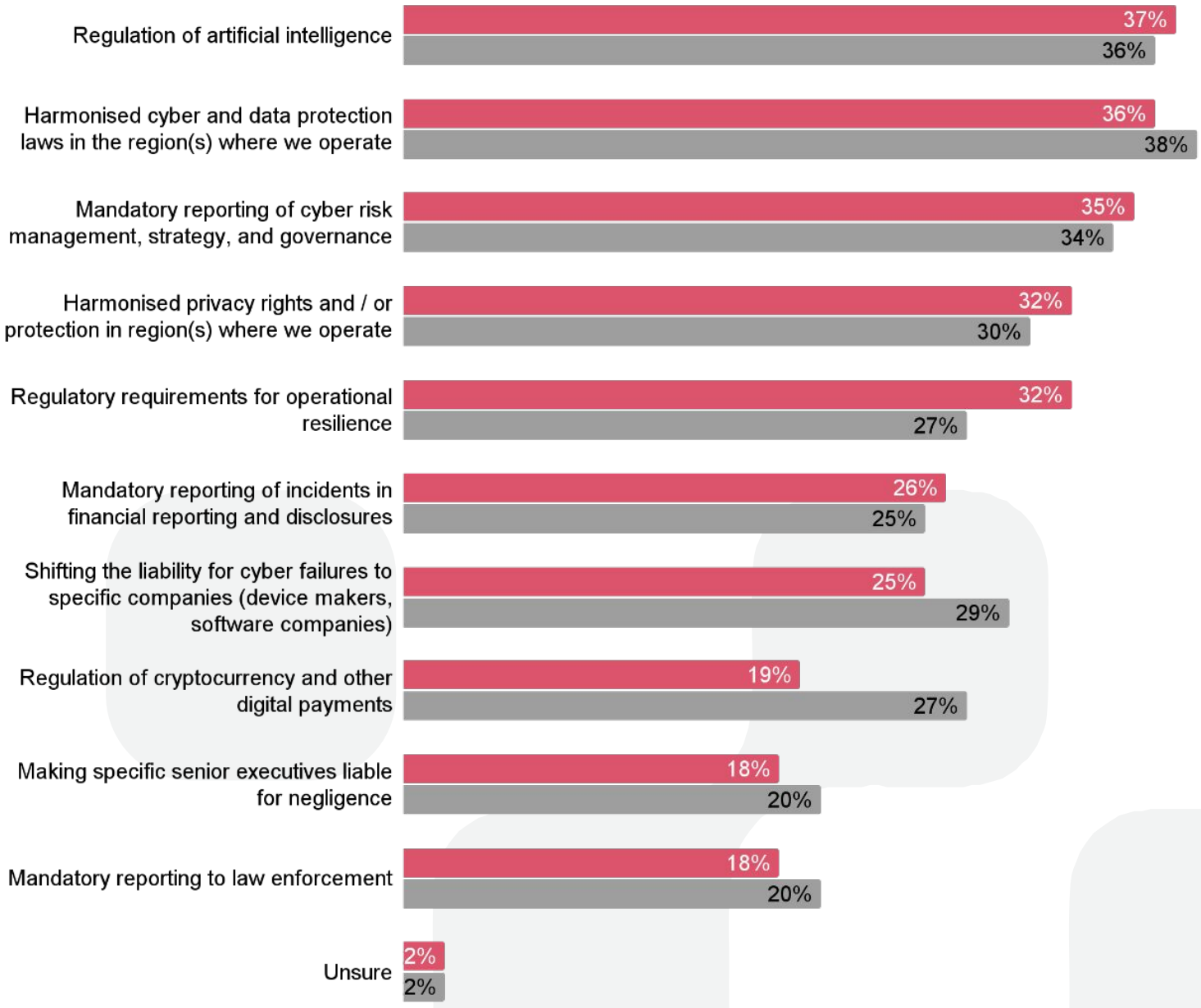
Cyber risk and incident reporting:
GenAI might also make cyber risk and incident reporting much simpler. With the help of natural language processing (NLP), GenAI can turn technical data into concise content that nontechnical people can understand. It can help with incident response reporting, threat intelligence, risk assessments, audits and regulatory compliance. And it can present its recommendations in terms that anyone can understand, even translating confounding graphs into simple text.

03

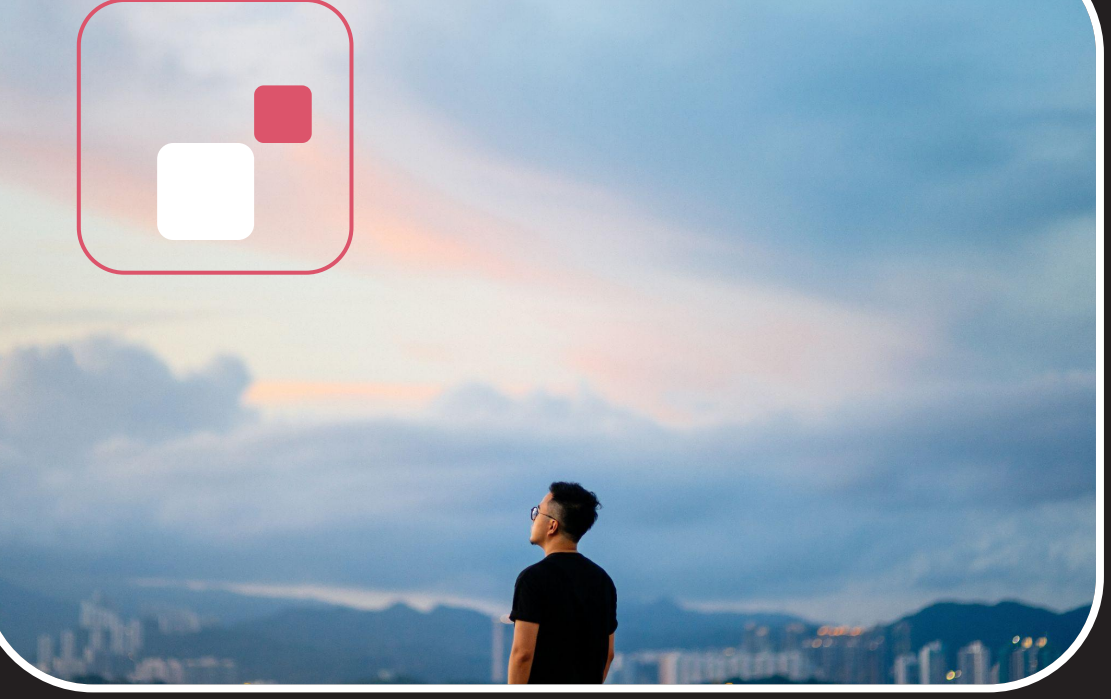
Adaptive controls:
Machine learning algorithms and GenAI tools could soon recommend, validate and draft security policies and automate controls that are tailored to an organisation's threat profile, technologies and business objectives.

Regulations: Providing a safe place to play and grow

About a third of this year's Middle East respondents agree that four types of regulation will be most important to securing the future growth of their organisation — harmonisation of cyber and data protection laws (38% vs 36% globally), regulation of AI (36% vs 37% globally), mandatory reporting of cyber risk management, strategy and governance (34% vs 35% globally)) and operational resilience requirements (27% vs 32% globally).



Question: Which of the following proposed regulatory goals and principles will have the greatest impact on your organisation's ability to secure future revenue growth?
Base: Global respondents = 3876, Middle East respondents = 110
Source: PwC, 2024 Global Digital Trust Insights



The way forward

In the region, as businesses continue to evolve, organisations must reconsider their cybersecurity strategies and adopt a new approach. As the global report highlights: "Innovation means making bold moves, and there's nothing more empowering than ensuring safety." Today, the integration of robust security measures and the fostering of digital trust is non-negotiable. Organisations need to act quickly, turning threats into opportunities for strengthening defences.

The Middle East findings of the 2024 Global Digital Trust Insights survey reveal that the discussion around cybersecurity now needs to move from the IT and security teams to the boardroom where leaders need to make cybersecurity a priority and strengthen the culture of cyber preparedness.

Business leaders are taking proactive measures to ensure cyber safety by staying ahead of cyber risks in line with global trends and business strategies. One of the trending directions in this pursuit is exploring advanced technologies like Generative AI, which can help anticipate cyber risks and strengthen security mechanisms.

Building a strong cyber resilience team is important, which can be achieved by bringing together individuals from cross-functional units such as cybersecurity, IT, and risk management. Furthermore, our survey showed that 36% of regional respondents have already implemented or experienced the benefits of using managed services in new areas, including security operations. This provides an opportunity for leaders to consider using managed services to strengthen their cyber resilience.

It is essential for leaders to foster collaboration among relevant stakeholders towards the implementation of cyber regulations that promote transparency and accountability. Leadership in the region must prioritise investments to secure the weakest links against cyber threats. With 77% of regional respondents increasing their cyber budgets, there is positive development in this sector and a clear indication that organisations are taking their cybersecurity goals seriously to tackle current and future challenges.

About the survey

PwC's Global Digital Trust Insights Survey has been running for 26 years and it is the longest-running annual survey on cybersecurity trends. It is also the largest survey in the cybersecurity industry and the only one that draws participation from senior business executives, not just security and technology executives.

The 2024 Global Digital Trust Insights is a survey of 3,876 business, technology and security executives (CEOs, corporate directors, CFOs, CISOs, CIOs and C-Suite officers) with over 100 respondents from the Middle East. The survey was conducted by **PwC Research**, PwC's global Centre of Excellence for market research and insight in the May through July 2023 period.

Contact us

Matthew White
Partner, Digital Trust and Cyber Leader
PwC Middle East
matthew.white@pwc.com

Haitham Al-Jowhari
Partner, Digital Infrastructure and Cybersecurity
PwC Middle East
haitham.al-jowhari@pwc.com

Oliver Sykes
Partner, Digital Trust | Technology Consulting
PwC Middle East
oliver.sykes@pwc.com

Ayesh
Director, Cybersecurity
PwC Middle East
mohammed.ayesh@pwc.com

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 152 countries with nearly 328,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com. Established in the Middle East for 40 years, PwC has 24 offices across 12 countries in the region with around 8,000 people. (www.pwc.com/me). PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

© 2023 PwC. All rights reserved.